Data protection: business development briefing

This business development briefing just provides an overview of the law in this area. You should talk to a lawyer for a complete understanding of how it may affect your particular circumstances.

This business development briefing highlights the key legal obligations a business should consider when dealing with personal data about customers, suppliers, employees and any other individual who may be encountered during the course of business.

Penalties for failing to deal with personal data appropriately

There could be serious financial, commercial and reputational implications for a business (including possible criminal penalties and fines) if personal data is not handled properly.

Protecting and securing personal data

Personal data is any information about an individual held on computer or in organised filing systems that could identify the individual, either on its own or together with other information held by a business or a third party. Personal data needs to be protected and kept secure. This data may include:

- Name.
- Email address.
- Telephone numbers.
- Date of birth.
- Notes written about someone (such as an annual performance review).

Particular care must be taken with sensitive personal data (for example, medical records) as more restrictive requirements apply to this type of data.

The individual could be a potential or actual employee, customer or supplier, or possibly someone captured on a business' CCTV footage.

Collecting personal data

A business can only collect personal data if it has a legitimate reason for doing so (for example, because a new employee is coming to work for the business).

When a business collects data about an individual, the business will need to tell that individual what it intends to do with their data (for example, if the business is collecting a customer's email address to confirm an order). If the purposes for which the business wants to use someone's data changes, the individual must be informed once again.

Businesses should only collect information they require at that particular time. For example, a job applicant should not be asked for their bank details. This type of data should only be collected once the applicant has started to work for the business.

If a business wants to use someone's data for marketing purposes, the individual must be informed. It is good practice to do this at the time the data is collected. In some cases (such as text or email marketing) a business will generally require the individual's explicit consent.

Using data collected on individuals

A business is generally allowed to use someone's personal data if they have given their consent. The data can also be used in other circumstances, for example, if the business:

- Needs to use the data to fulfil a contract with a customer (such as using their address to deliver goods to them).

- Has a legitimate interest in using it, although this must be balanced with the individual's rights. For example, if a part of a business has been sold to a third party and the business needs to transfer customer data to it.

Data should only be used for the reason that it was collected (for example, if calls between staff and customers are recorded for training purposes only, they should not be used to discipline a member of staff).

If a business wants a third party to manage data (such as carrying out payroll services) it should take legal advice. The business will still be responsible for protecting the data and will need to enter into a written contract with the third party.

Businesses should take legal advice if they are considering transferring any data outside the countries in the European Economic Area. It is very easy to transfer data outside the country a business is based in (for example, by sending an email to an office outside the UK).

If the data is being used in marketing material, businesses should check that the recipient is aware that their data may be used for this reason and confirm they do not object. A business will generally need the individual's explicit consent (opt-in) for email, fax and text marketing. If the individual is an existing customer, the business may be able to market similar products to them by these means without prior explicit consent. Businesses should take legal advice in these circumstances.

If a business is considering using sensitive personal data, it should take legal advice (for example, information about ethnic origin, trade union membership or criminal records).

Storing personal data

All data must be accurate and up to date. Databases should be regularly cleaned and out-of-date information must be deleted.

Data should only be held for as long as it is required and for the reason it was collected. For example, if personal data was collected to deliver a product a year ago and has not been used since, it should not be held on the basis that it may be needed for another reason at some time in the future.

Keeping data secure and confidential

Personal data must be kept secure at all times. For example:

- Computers and files should be password protected.

- Personal data on laptops and other portable devices should be kept to a minimum.

- Manual filing cabinets containing personal data should be locked and only accessible to authorised personnel.

- Confidential documents should not be left unattended on desks.

- Personal data should be removed promptly from fax machines, printers and photocopiers.

- Ensure staff are appropriately trained to handle personal data safely and securely.

When a business sends personal data, it must be done in a secure way (for example, confidential information should not be sent in the internal mail).

Personal data must be disposed of securely (for example, by shredding, placing in confidential waste bags, destroying or securely deleting electronic files). Confidential papers should not be put in the recycling bin.

Security breaches (such as accidentally losing personal data) should be reported to the appropriate person immediately.

Electronic documents, including calendar entries and meeting requests, should be password protected or designated private where appropriate.

Working away from the office

When working away from the office or in public areas:

- Ensure personal data stored on portable devices such as laptops, Blackberries, tablets or memory sticks is encrypted and kept secure at all times.
- Avoid leaving papers or electronic devices lying around.
- Make sure members of the public cannot see confidential documents or computer screens; and
- Avoid talking about confidential matters when members of the public may be able to hear.

Enquiries about personal data

Businesses should have a system in place to deal with individuals who request details of the personal information that the business holds on them. A business is permitted to charge an administration fee of up to £10 for responding to this type of request.

Individual employees should not deal with this type of enquiry, unless they have been given specific authorisation to do so. The request should normally be passed to the person within the business who has responsibility for data protection issues.

Personal data should not be given out to the friends or relatives of an individual without that individual's specific consent.